**Management Advisory Report: Review of
Lost or Stolen Sensitive Items of Inventory
at the Treasury Inspector General for Tax
Administration**

May 2002

Reference Number: 2002-10-108

INSPECTOR GENERAL
for TAX
ADMINISTRATION

May 31, 2002

MEMORANDUM FOR THE TREASURY INSPECTOR GENERAL FOR TAX
ADMINISTRATION

FROM: Pamela J. Gardiner
                   Deputy Inspector General for Audit

SUBJECT: Final Management Advisory Report - Review of Lost or Stolen
                  Sensitive Items of Inventory at the Treasury Inspector General
                  for Tax Administration (Audit # 200210012)

This report presents the results of our review of the effectiveness of the Treasury
Inspector General for Tax Administration's (TIGTA) inventory controls over firearms,
computers, and other sensitive items that, if lost or stolen, might compromise the
public's safety, national security, or ongoing investigations. This review was conducted
at the request of Senator Charles E. Grassley, Ranking Member of the Senate
Committee on Finance.

In summary, we found that the TIGTA has established or is in the process of developing
procedures to control its inventory of computers, firearms, and other sensitive items of
inventory. However, its inventory procedures over the accountability of computers could
be improved by providing guidance as to when lost or stolen computers should be
referred for investigation. Further, physical inventories to account for its inventory of
computers were not regularly performed.

In addition, the data recorded in its inventory systems proved to be insufficient to
adequately control its inventory of computers, firearms, and other sensitive items of
inventory. The TIGTA is working to implement a new inventory system to accurately
account for and control its property and equipment. For the past 3 years, the TIGTA
reported 4 stolen computers, 2 computers lost during delivery, and 44 unaccounted for
computers resulting from physical inventories. TIGTA's Office of Information
Technology subsequently located 13 of the 44 missing computers. All but 2 of the
remaining 31 missing computers were obsolete at the time the inventory was taken.
TIGTA also reported no lost or stolen firearms; however, it did report 22 other

investigative items that were lost or stolen. Further, the TIGTA reported that no missing computer contained classified data, or had an internal secure modem installed.

Management's Response: TIGTA management agreed to the recommendations presented in the report. They plan to implement an integrated inventory system that will allow TIGTA to easily, effectively, and efficiently maintain inventory control over firearms, computers, and all other items required by statute or policy before the end of the year. The TIGTA Personal Property Management Officer will be responsible for assuring the integrity of the inventory system. Further, the TIGTA inventory system has been added to the Office of Information Technology Program Status Review list, and the TIGTA will regularly monitor the program status review list, and formally review it on a quarterly basis. Management's complete response to the draft report is included as Appendix IV.

Please contact me at (202) 622-6510 if you have questions or Daniel R. Devlin, Assistant Inspector General for Audit (Headquarters Operations and Exempt Organizations Programs), at (202) 622-8500.

Table of Contents

Management Advisory Report: Review of Lost or Stolen Sensitive Items of Inventory at the Treasury Inspector General for Tax Administration

Background	This review was conducted at the request of Senator Charles E. Grassley, Ranking Member of the Senate Committee on Finance. Senator Grassley, in a letter dated September 25, 2001, voiced concerns over the controls within the Internal Revenue Service (IRS) to effectively perform its mission while protecting the integrity of its inventory of sensitive items. For purposes of his request, he defined inventory to include the IRS' stock of firearms, computers, and other items that, if lost or stolen, might compromise the public's safety, national security, or ongoing investigations. A subsequent request was made for a similar review at the Treasury Inspector General for Tax Administration (TIGTA).

Our review was conducted at the TIGTA National Headquarters in Washington, D.C. during the period September through November 2001, and included the Office of Investigations (OI) and the Office of Information Technology (OIT). The audit was conducted in accordance with the President's Council on Integrity and Efficiency's *Quality Standards for Inspections*. Though the Office of Audit is part of the TIGTA organization, we believe that our independence in conducting this review was not adversely affected. Organizationally, the Offices of Audit, Investigations, and Information Technology, have separate reporting responsibilities to the Inspector General, who is responsible for the overall operation of the organization. Detailed information on our objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

During the review, we coordinated our work with the Department of the Treasury Office of Inspector General (OIG) and the General Accounting Office (GAO), both of whom are performing similar reviews of sensitive inventory items in other Treasury bureaus and government agencies, respectively.

In his request, Senator Grassley asked that the TIGTA include in its assessment the following six elements:

- Evaluate whether the TIGTA's inventory regulations are sufficient to prevent loss or theft of its inventory.

- Identify any missing or stolen item of TIGTA inventory for the past 3 years, to include that item's description and a brief explanation of the loss.

- Evaluate the TIGTA's plan to recoup inventory that cannot be located for the past 3 years.

- Recommend methods to improve the TIGTA's inventory regulations and accounting methods to prevent future loss.

- For any missing computer, state whether the computer contained classified data. In general terms, describe the nature of that data. Also, describe the TIGTA's plan to prevent the unauthorized dissemination of such data.

- For any missing computer, state whether the computer had an internal secure modem that allowed access to internal networks. If so, state the number of missing computers that allowed for such access. Also, describe the TIGTA's plan to prevent unauthorized access to internal networks.

We are presenting the results of our review by separately addressing each of these six elements. The information and data we obtained are what the TIGTA has reported to us, and we did not independently verify the data; accordingly, we express no opinion on the accuracy or completeness of the data.

Evaluation of the Treasury Inspector General for Tax Administration's Inventory Regulations

The TIGTA has established or is in the process of developing procedures to control its inventory of computers, firearms, and other sensitive items of inventory. However, its inventory procedures over the accountability of computers could be improved by providing guidance as to when lost or stolen computers should be referred for investigation. Further, physical inventories to account for its inventory of computers were not regularly performed.

In addition, the data recorded in its inventory systems proved to be insufficient to adequately control its inventory of computers, firearms, and other sensitive items of inventory.

Computers

In October 1999, the TIGTA discontinued use of the IRS' asset management system called the Integrated Network and Operations Management System (INOMS). A download of TIGTA computer inventory was obtained from the INOMS and later transferred to an inventory system called BarScan without any significant cleanup of the data being transferred. The TIGTA did not conduct any physical inventories of this data. The last physical inventory that was conducted was in 1999 in conjunction with its computer readiness efforts for the year 2000. During the transfer of data and Year-2000 readiness physical inventory, any computer equipment that could not be located was coded as "16" (Pending Resolution), with no efforts made to resolve these items in the inventory records. No items were recorded in the inventory as "07" (Lost/Theft/Damaged). Further, the TIGTA's procedures did not include guidance on how to report or refer for investigation items of missing inventory.

In October 2001, new procedures were developed for the overall inventory process within the TIGTA. Procedures for accounting and controlling computer equipment from procurement to disposal were established in the TIGTA manual. Further, the TIGTA plans to replace the BarScan system with an integrated inventory system to account for all TIGTA equipment and property, including computer equipment. The TIGTA will start implementing the system during the first quarter of Fiscal Year 2003.

As part of the new procedures, the Assistant Inspector General for Information Technology (AIGIT) is responsible for a Personal Property Management Program. The AIGIT has also designated a Personal Property Management Officer (PPMO) to oversee the property management program and the inventory system.

On an annual basis, TIGTA managers are to receive an inventory list of personal property assigned to their office or employees. They are to review the list and certify to its accuracy. The certifications are to be provided to and maintained by the PPMO. Further, the PPMO is to conduct periodic physical inventories to both verify the data

recorded in the inventory system and to validate the certifications submitted by the responsible manager. All results will be reported to the appropriate TIGTA executive.

The procedures also require all employees to report property that has been lost, stolen, or damaged to their managers and the PPMO within 48 hours. The reports are to be written memoranda and should include the type of property, serial number, a description of the circumstances surrounding the loss, and a description of the efforts taken to retrieve the property. However, the procedures, as written, do not require nor provide guidance on reporting lost or stolen items of inventory to the TIGTA's OI for investigation.

Firearms and Other Sensitive Items

The Assistant Inspector General for Investigations, Technical and Forensic Support Division, is responsible for maintaining an inventory of all investigative equipment. Investigative equipment includes, but is not limited to, the following:

- Firearms.

- Body Armor.

- Radio communication equipment.

- Electronic surveillance equipment.

- Vehicles.

- Badges/Credentials.

During the period of our review, the OI used an on-line inventory management reporting system called the Automated Control of Equipment and Supplies (ACES) system to control its inventory of investigative equipment. Procedures for the investigative equipment inventory process from procurement to disposal were established in the TIGTA manual. These procedures call for the recording of all investigative equipment to include its description, assigned individual, location, manufacturer, model, serial number, date acquired, and cost. However, when asked to provide a download of all lost or stolen investigative equipment for the past 3 years from the ACES system, the

OI informed us that the data might not be reliable since the ACES has no data field to identify lost, stolen, or destroyed items of inventory. This necessitated the OI to manually identify these items. As with the computer inventory, the TIGTA plans to replace the ACES system during the first quarter of Fiscal Year 2003 with an integrated inventory system to account for all TIGTA equipment and property, including investigative equipment.

OI's inventory procedures require each Special Agent in Charge (SAC) to conduct a physical inventory of all investigative equipment annually. As part of the inventory process, a reconciliation is performed between what is inventoried and what is recorded on the ACES. The SAC is required to submit a memorandum to the Deputy Inspector General for Investigations (DIGI) certifying that all investigative items are present and to advise of any discrepancies not reconciled during the inventory.

The SAC is also required to provide an annual certification that the inventory and reconciliation process was completed. Inventory certifications were completed for 2001. Further, the Special Inquires and Inspection Division is required to perform a review to verify and validate that the annual inventories and related certifications are performed.

OI's inventory procedures require that any lost, stolen, damaged, or destroyed property be reported using a *Report of Survey* (Form 1933). The form is to be sent to the Technical and Forensics Support Division for review. After review, the form is to be forwarded to the Headquarters Property Officer for final determination.

Identification of Missing or Stolen Items of the Treasury Inspector General for Tax Administration's Inventory

Our reporting of lost or stolen items involved the period October 1, 1998, through September 30, 2001, unless otherwise noted. Also, the TIGTA had inventory located in buildings impacted by the terrorist activities of September 11, 2001; accordingly, some numbers may not have been updated to reflect those events.

Computers

It was the OIT's practice to leave missing computers on its inventory system as a status code 16 instead of removing the computers from the inventory. Further, no efforts were

made to update the inventory records to record items into status code 07 where warranted. Therefore, specific numbers differentiating between lost or stolen computers, or eliminating damaged or obsolete computers, could not be provided through the inventory records.

For the OIT to provide the number of lost or stolen computers for the past 3 years, it had to perform an analysis of its manual and electronic records about missing or stolen computers. Based on their analysis, OIT personnel reported 50 missing computers. However, OIT stipulated in its reporting that information older than 18 months yielded data of inconsistent validity, and cannot be relied upon for accuracy. The reporting detailed 4 stolen computers, 2 computers lost during delivery, and 44 computers unaccountable during physical inventory as follows:

- On April 18, 2001, an employee's vehicle was broken into and a laptop computer was stolen. The incident was reported to the local police and to the TIGTA's OI. The computer was not recovered. The employee was counseled concerning the incident. This computer was acquired in June 1999 for approximately $3,100, and at the time of loss, had an approximate depreciated value of $1,400.

- On December 1, 2000, a TIGTA office was broken into and two laptop computers were stolen. The incident was reported to the local police and to the TIGTA's OI. An investigation was conducted by the TIGTA's OI and the case was closed without recovery of the missing computers. No disciplinary action was deemed necessary by the TIGTA in this incident. These computers were acquired in June 1999 for approximately $6,300 and at the time of loss, had an approximate depreciated value of $3,400.

- In September 1999, an employee's vehicle was broken into and a laptop computer was stolen. The incident was reported to the local police and to the TIGTA's OI. Based on the circumstances surrounding the incident, the OI did not pursue an investigation. No disciplinary action was deemed

necessary by the TIGTA in this incident. This computer was acquired in June 1999 for approximately $3,100, and at the time of loss, had an approximate depreciated value of $2,900.

- In January 2000, two computer network servers were identified as missing when several system packages were shipped from certain field offices to the TIGTA's Headquarters Office. When questioned at the time, the affected field office explained that the missing computers were never received during the initial shipment in late 1998. The incident was not reported to the local police or to the TIGTA's OI. No disciplinary action was identified concerning this incident. These computers were acquired in December 1998 for approximately $14,400, and at the time of loss, had an approximate depreciated value of $9,600.

- In December 1999, 44 computers could not be located during the TIGTA's 1999 Year-2000 readiness inventory. As part of our review, the OIT reported on November 27, 2001, that the missing computers were determined to be obsolete and to have no residual value; therefore, no referral was made for investigative purposes and no disciplinary actions were taken. A further analysis of the OIT-provided documentation by the auditors showed that 13 of these computers were approximately 1 year old or less when the readiness inventory was taken. These 13 computers had an approximate acquisition cost of $51,000. After reporting this condition, the OIT conducted another search and subsequently located 11 of the 13 computers,[1] as well as two additional computers that were classified as obsolete. The OIT advised that it will continue actions to locate the remaining 2 of 13 computers. These 2 computers had an approximate acquisition cost of $7,400, and a depreciated value of approximately $4,900 at the time the loss was discovered.

---

[1] We physically verified the existence of the first eight computers that the OIT subsequently located.

As of November 26, 2001, the OIT reported that it had approximately 1,380 in-use computers, and 200 computers used as network system servers in its inventory. The TIGTA employs approximately 950 professionals that make use of these computers.

Firearms and Other Sensitive Items

The OI staff informed us that they could not rely on the ACES system to provide a reasonably accurate extract of the number of lost or stolen items of investigative equipment for the past 3 years. This was due to an overall lack of confidence in the system to provide such an extract since the system does not contain a data field designating items as lost or stolen. As an alternative, the OI staff reviewed investigative files to identify lost or stolen items. They also canvassed field office and Headquarters employees to identify any lost or stolen equipment that may not have surfaced through the investigative files analysis.

As a result of these efforts, the OI reported no lost or stolen firearms in the past 3 years. However, it did report 22 other investigative items that were lost or stolen in the past 3 years. Included in the 22 other items were a lost law enforcement raid badge and raid jacket that, if used by an unauthorized individual, could possibly compromise the public's safety or ongoing investigations.

The remaining 20 investigative items included the following:

- In June 1999, three portable radios were stolen after an employee inadvertently left them on the sidewalk. All appropriate local and national law enforcement agencies, and the manufacturer were notified. The TIGTA's OI reviewed the incident without recovery of the property. There was no indication of any disciplinary action in this case.

- In August 2000, a cellular telephone, a pair of binoculars, and a law enforcement baton were stolen from an employee's vehicle. The TIGTA's OI investigated the incident without recovery of the property. There was no indication of any disciplinary action in this case.

- In January 2001, nine portable radios and a cellular phone were stolen from a locked government surveillance van. The break-in and the theft were reported to local police, and the local TIGTA Field Division undertook a companion investigation without recovery of the property. Although there was no indication of any disciplinary action in the case information provided, we were advised in management's response that oral counseling, confirmed in writing, was administered.

- The remaining items included a receiver device, a camera lens, a video camcorder, and a pocket television that were unaccounted for after physical inventories.

The OI also reported that two government-owned vehicles were stolen during the past 3 years, but were subsequently recovered.

Although the OI's procedures require the preparation of Forms 1933 to document and report missing items of inventory, none were prepared for the above items. Instead, OI agents usually prepared memoranda that included the details of the incidents.

The OI further reported no lost or stolen items of seized property for the past 3 years.

As of September 30, 2001, the OI reported that it had approximately 850 firearms in its inventory. These included standard duty handguns issued to each Special Agent (SA); one extra-unassigned handgun for every 5 to 10 SAs; special duty handguns for undercover, training, and competition; shotguns for each group/post-of-duty; law enforcement rifles; and, firearms maintained for training purposes. The TIGTA employs approximately 360 SAs located in approximately 70 posts-of-duty.

Evaluation of the Treasury Inspector General for Tax Administration's Plan to Recoup Inventory

In general, the TIGTA has made efforts to recoup missing computers and other sensitive items. However, efforts to investigate computers missing during delivery and computers identified as missing during physical inventories could have been more comprehensive to fully determine the status of the missing computers.

Computers

Though no formal reporting procedures existed in the TIGTA's manual during the period of our review, the four stolen computers were referred to local police and the TIGTA's OI for investigation. However, no referral was made for the 2 computers that were lost during delivery or the 44 computers that could not be located during the TIGTA's 1999 Year-2000 readiness inventory. OIT management explained that the two lost computers were not referred for investigation due to the circumstances surrounding the incident. Further, the 44 computers were not referred for investigation, since they determined the computers to be obsolete and having no residual value.

Firearms and Other Sensitive Items

Fourteen of the 22 lost or stolen items of investigative equipment were formally investigated by the TIGTA's OI. Items not referred for investigation were determined not to warrant such action due to the circumstances surrounding the incidents.

As mentioned earlier, the TIGTA's OI along with local police were successful in recovering two stolen government owned vehicles.

Recommendations to Improve the Treasury Inspector General for Tax Administration's Inventory Regulations

Based on our limited review, we recommend that the TIGTA take the following actions:

Recommendations

1. Establish specific status codes to differentiate between lost, stolen, and damaged items of inventory for the new TIGTA inventory system.

Management's Response: The new TIGTA Personal Property Module (PPM), part of the TIGTA's Performance and Results Information System (PARIS), has been designed to maintain comprehensive information about each inventory item. The system provides a status indicator on whether the inventoried item is lost, stolen, or damaged as well as the ability to further define other status indicators (e.g., in repair, seized, pending sale).

2. Periodically generate from the inventory system a report of all items of inventory that are recorded as status code "16" to ensure prompt and accurate action on these items, including a full investigation when warranted.

Management's Response: The TIGTA has discontinued use of status code "16," and the new PPM will not contain indefinite codes like "16" to track the status of inventory items. Each code will clearly indicate the true status of each item, and require appropriate action dictated by the code. These actions will be performed at the time the code is set. The TIGTA Board of Survey will determine status codes that require full investigation.

3. Provide written guidance on the types of lost or stolen equipment, including items identified during physical inventories, which should be referred to the TIGTA's OI for investigation.

Management's Response: The TIGTA has issued written guidance in the TIGTA Operating Manual, Chapter 500, Section 140, which outlines the proper procedures for reporting all types of lost or stolen equipment. Augmenting this guidance, in-house training for all staff with inventory responsibility has commenced. In addition to instruction in the operation of the new PPM, this training will include awareness training in the application of TIGTA property management policy and employee responsibilities. Whenever an inventory item's status code is changed to reflect it has been reported missing, actions will be taken as determined by the TIGTA Board of Survey, including referral for full investigation.

4. Ensure that periodic physical inventories are performed on the inventory of computers and that all discrepancies are resolved.

Management's Response: Guidance has been included in the TIGTA Operating Manual stipulating annual physical inventories be conducted throughout the organization. In addition to conducting routine physical inventories, managers will be required to certify inventory lists of all items assigned to them and their staff. The TIGTA Personal

Property Management Officer will report any discrepancy to the Chief Information Officer and if necessary, a meeting will be convened of the TIGTA Board of Survey. The TIGTA will conduct a comprehensive physical inventory beginning October 1, 2002.

5. Reinforce the guidelines to prepare Forms 1933 to consistently report lost or stolen items of inventory, or revise the guidelines if a comparable form of documentation is deemed appropriate.

Management's Response: As stipulated in the guidelines of the Operating Manual, the TIGTA uses a process for consistently reporting and documenting lost or stolen items of inventory. The guidelines include how employees should report lost, stolen or damaged property. Potential disciplinary actions for lost or stolen items are outlined in the guidelines. The TIGTA Board of Survey will ensure consistent application of recommendations of disciplinary action across the functions. Guidelines in the TIGTA Operating Manual will be reinforced during the training mentioned above to assure consistency. In addition, the TIGTA will amend Form 1933 to more accurately reflect the appropriate reporting requirements for firearms and sensitive items lost, stolen, or damaged.

6. Develop an encryption policy to reduce the risk of unauthorized disclosure of sensitive information maintained on laptop computers.

Management's Response: The TIGTA is participating in a Treasury information technology program piloting the use of Private Key Infrastructure (PKI) and smart cards. It is essential for the interoperability of the TIGTA's systems with the Treasury Department that the TIGTA take advantage of this enterprise solution. Coincident with the pilot, that begins July 1, 2002, will be the development of an encryption policy to reduce the risk of unauthorized disclosure of sensitive information maintained on laptop computers.

Missing Computers Containing Classified Data or Taxpayer Information

The TIGTA reported that no lost or stolen computers contained classified data. All classified data in the possession of the TIGTA, at the time of our review, was reported to be hardcopy material and was maintained in safes. The TIGTA has a policy that no classified data be maintained on an employee's computer.

Further, the TIGTA reported that 1 of the stolen computers did not contain taxpayer information, but was unable to confirm through documentation whether the remaining 49 (3 stolen, 2 lost during delivery, and 44 not located during inventory) computers contained taxpayer information. Though documentation was not available, the TIGTA believes that none of the 49 computers contained taxpayer information.

The TIGTA has no written encryption policy to protect sensitive but unclassified information, such as taxpayer information, maintained on its laptop computers. Though the maintenance of taxpayer information on laptop computers is not a common practice within TIGTA as a whole, taxpayer information is, at times, maintained on laptop computers, especially within the Office of Audit. The Office of Audit does employ an audit software package that provides encryption when using certain applications controlled within the package. However, there is no requirement that all sensitive files be maintained using either the audit software package or the specific applications that invoke the encryption process.

To prevent unauthorized access to programs and files maintained on TIGTA laptop computers, the TIGTA makes use of an operating system password access control. By using this method, an employee must have a system-recognized login name and password to gain access to the computer. Though this control does provide a deterrent to prevent an unauthorized individual from powering-up the computer and accessing programs and data through the computer's installed operating system, it can be compromised to gain access to unencrypted files maintained on the computer's hard drive by a knowledgeable and determined individual.

The ability to gain access in this manner increases the vulnerability of unauthorized disclosure of sensitive information if a laptop computer is lost or stolen, and further necessitates the need to encrypt all files that contain such information.

Missing Computers With Access to Internal Networks

The TIGTA does not use any modems that would be termed an internal secure modem. Therefore, access to TIGTA networks through any missing computers is unlikely. To gain access to TIGTA networks or internal database systems, one must first be able to logon to the computer itself. This entails the use of a username and password. However, as previously mentioned, a knowledgeable and determined individual may be able to gain access. But, once into the TIGTA's intranet, the individual would not only have to go through an additional logon process for a given system, but would also have to be recognized by that system as a person authorized to gain access.

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine the effectiveness of the Treasury Inspector General for Tax Administration's (TIGTA) inventory controls over firearms, computers, and other sensitive items that, if lost or stolen, might compromise the public's safety, national security, or ongoing investigations. In doing so, we gathered sufficient evidence to specifically answer the questions posed in the congressional request, including the identification of any missing or stolen items for the past 3 years. To accomplish our objective, we:

I.   Developed an understanding of the TIGTA's policies and procedures for managing and controlling its inventory of sensitive items, including procedures to prevent the loss or theft of such items.

   A. Obtained current inventory procedures for recording, safeguarding, and disposing of inventory items. Discussed procedures with responsible TIGTA officials to ensure our understanding of the procedures.

   B. Identified controls to ensure that policies and procedures were followed.

   C. Identified the procedures to report missing or stolen property.

   D. Identified the procedures to recover any missing or stolen property.

II.   Determined whether the TIGTA's policies and procedures for managing and controlling sensitive items, including procedures to prevent the loss or theft, were effective.

   A. Evaluated the procedures and controls with regards to providing an inventory process that is reasonable and that would provide for effective accountability to prevent the loss or theft of sensitive items such as firearms, computers, etc.

   B. Obtained summary inventory listings of all property, and identified items that, if missing or stolen, might compromise the public's safety, national security, or ongoing investigations.

   C. Obtained a listing of any missing or stolen items of inventory (including all seized property) for the past 3 years (October 1, 1998, to September 30, 2001), and attempted to obtain documentation to identify the item's description and explanation of the loss.

   D. Identified if any missing computers contained classified data and/or internal secure modems that would either allow for unauthorized dissemination of data or access to internal TIGTA networks. Also, identified the TIGTA's plans to prevent such unauthorized activity.

1. Inquired of the TIGTA as to whether any classified data existed within the agency, and if so, the location of such data.

2. Documented the process to gain access to TIGTA automated systems through dial-in procedures.

E. Evaluated the results of any efforts to recover missing or stolen items.

F. Obtained physical inventory records to evaluate the extent of the inventories and to see if sensitive types of items were being identified during the physical inventory process.

Major Contributors to This Report

Daniel R. Devlin, Assistant Inspector General for Audit (Headquarters Operations and Exempt Organizations Programs)
John R. Wright, Director
Thomas J. Brunetto, Audit Manager
S. Kent Johnson, Senior Auditor
Bobbie M. Draudt, Auditor
Peter L. Stoughton, Auditor
Nikura M. Thomas, Auditor

Report Distribution List

Deputy Inspector General for Investigations IG:I
Assistant Inspector General for Information Technology IG:IT

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

RECEIVED
MAY 2 3 2002

May 23, 2002

MEMORANDUM FOR THE DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: David C. Williams
                  Inspector General

SUBJECT: Response to Draft Management Advisory Report – Review of
                  Lost or Stolen Sensitive Items of Inventory at the Treasury
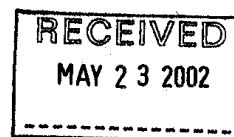   Inspector General for Tax Administration (TIGTA) Audit
                  #200210012

I appreciate the opportunity to respond to the above referenced report, and supply additional information on the subject matter. As noted in the report, we are improving the accountability of our inventory system, policy and guidance. We will assure that your recommendations are incorporated in these changes. As a priority, we are implementing an integrated inventory system that will allow TIGTA to easily, effectively and efficiently maintain inventory control over firearms, computers, and all other items required by statute or policy before the end of the year. The TIGTA Personal Property Management Officer will be responsible for assuring the integrity of our inventory system. Further, the TIGTA inventory system has been added to the Office of Information Technology Program Status Review list, and TIGTA will regularly monitor the program status review list, and formally review it on a quarterly basis

Investigative Equipment
Notwithstanding that the Office of Investigations was able to furnish a full accounting of all lost, stolen and destroyed items during the period under analysis, we are fully committed to ensure the effective and efficient accounting of all firearms, and other sensitive inventory items entrusted to our care.

Form 1933, Report of Survey, is referenced within Section 160.7.10 of the TIGTA Investigations Manual Chapter 400 as the means by which lost, stolen or damaged items are to be reported. However, field and headquarters divisions typically employ an official memorandum to convey the full circumstances surrounding such losses and the investigative steps taken to recover/report items via the National Crime Information

Center (NCIC). Form 1933 is styled toward final disposition of property rather than the full scope of information surrounding its loss. Consequently Form 1933 is an inefficient artifact of the legacy system that TIGTA utilizes to track investigative property. TIGTA will amend Form 1933 to more accurately reflect the appropriate reporting requirements for firearms and sensitive items lost, stolen or damaged. The responsible Assistant Inspector General for Investigation will forward the amended form 1933 via official memorandum to the TIGTA Personal Property Management Officer (PPMO) thus ensuring that the TIGTA Personal Property Management System is updated. The PPMO is the sole official vested with the necessary security permissions to enter such changes in status for inventory items. The PPMO would subsequently notify the program manager responsible for the investigative equipment item of the status change (e.g., firearms, radio communications, technical investigative equipment). Updates to reflect the manner and effects of changes will be made to the Investigations Manual by August 31, 2002.

The Assistant Inspector General for Investigations overseeing both the Operations Division and the Technical and Forensic Support Division is the official responsible for ensuring these actions. The PPMO will receive all official memorandums related to lost, stolen or destroyed investigative property and will constantly monitor the new system.

In addition to the above response, three statements contained in the subject report require clarification:

1. The report's section entitled, *Evaluation of the Treasury Inspector General for Tax Administration's Inventory Regulations*, at page four (4) states;

   "However, when asked to provide a download of all lost or stolen Investigative equipment for the past 3 years from the ACES system, the OI informed us that the data might not be reliable. This necessitated the OI to manually identify these items."

The ACES system has no data field to capture lost, stolen or destroyed equipment status information. This should not, however, suggest that the ACES inventory system, as a whole, is unreliable. As noted in the draft report, the Office of Investigations conducts annual physical inventories of all firearms, radio communications and technical investigative equipment. These physical inventories are reconciled with the data maintained in the ACES system each year. While the ACES system has no data field set apart to <u>automatically</u> identify lost, stolen or destroyed items, the Office of Investigations was able to provide such documentation based upon the findings of its annual physical inventory of investigative property. The ACES legacy system is old and inefficient, not inaccurate. Because ACES is based upon old proprietary protocols, it lacks state-of-the-art relational database search engines to generate sophisticated reports. The new PARIS Personal Property Management System, however, has specific data fields and audit trail capabilities to track lost, stolen and destroyed items.

Page 2

Moreover, the new PARIS Personal Property Management System can generate a wide variety of reports.

2. The report's section entitled, *Evaluation of the Treasury Inspector General for Tax Administration's Inventory Regulations*, at page eight (8) states;

   "The OI staff informed us that they could not rely on the ACES system to provide a reasonably accurate extract of the number of lost or stolen items of investigative equipment for the past 3 years due to an overall lack of confidence in the system."

As noted previously, the ACES system has no data field to capture lost, stolen or destroyed equipment status information. Rather than provide *reasonably accurate* data from an ACES query alone, the Office of Investigations went to the original source documents (memoranda) to substantiate lost, stolen or destroyed items. The lack of confidence in the ACES database relates to the specific data field to be searched and should not be misunderstood as a lack of confidence in the ability of the ACES system in general.

3. The report's section entitled, *Evaluation of the Treasury Inspector General for Tax Administration's Inventory Regulations*, at page eight (8) states;

   "In January 2001, nine portable radios and a cellular phone were stolen from a locked government surveillance van... There was no indication of any disciplinary action taken."

It should be noted that oral counseling, confirmed in writing, was administered to the employee involved after consultation with TIGTA's Personnel Management Specialist. Information related to administrative action taken against employees involved in the loss of investigative property would not normally be included in the original memorandum reporting the loss, theft or destruction of the item. Follow-up inquiry of each division SAC would be required to accurately determine what disciplinary action, if any, was taken. As noted in the above example, disciplinary action was taken.

Computers
The 44 computers initially reported as unaccounted for in the December 1999 Year 2000 readiness inventory were of two types, personal computers (PCs) and servers. One computer was a server and the remaining 43 were personal computers that can be divided into two further types; those that were already obsolete as of December 1999 (the date of the inventory), and those that were usable. 31 PCs fall into the former category with 12 PCs falling into the latter category, usable as of December 1999.

Page 3

Since issuance of the subject report, the server, ten of the twelve PCs usable as of 12/1999 and two PCs obsolete as of 12/1999 have been found. All of the computers that have been found were either in TIGTA spare parts storage waiting to be excessed or at the Federal Law Enforcement Training Center in Glynco, Georgia.

Type of computer	Number initially report unaccounted	Number found	Total still unaccounted
Server	1	1	0
PCs usable as of 12/1999	12	10	2
PCs obsolete as of 12/1999	31	2	29

Recommendations

1. *Establish specific status codes to differentiate between lost, stolen, and damaged items of inventory for the new TIGTA inventory system.*

Reasonable inventory procedures were not followed when setting the status codes for missing computers. This was due in part to the urgency generated by Year 2000 readiness preparations, resource constraints and an unwieldy inventory system inherited from the IRS. We are in the process of replacing several disparate inventory systems that require significant manual intervention to extract limited information about items under control. The new TIGTA Personal Property Module (PPM), part of our Performance and Results Information System (PARIS), has been designed to maintain comprehensive information about each inventory item. The system provides a status indicator on whether the inventoried item is lost, stolen or damaged as well as the ability to further define other status indicators (e.g., in repair, seized, pending sale). The system is flexible and will allow the addition of new codes as TIGTA's Property Management Program evolves. Further, the PPM system has been designed so that only the TIGTA Personal Property Management Officer is authorized to input the final disposition of all inventory items. The new system will be operational by September 30, 2002, and will be the responsibility of the PPMO.

Page 4

2.   *Periodically generate from the inventory system a report of all items of inventory that are recorded as status code "16" to ensure prompt and accurate action on these items, including a full investigation when warranted.*

TIGTA has discontinued use of status code "16", and the new PPM will not contain codes like the ambiguous "16" to track the status of inventory items. Each code will clearly indicate the true status of each item, and require appropriate action dictated by the code.   These actions will be performed at the time the code is set. The TIGTA Board of Survey will determine status codes that require full investigation.   The TIGTA Board of Survey is composed of TIGTA's Senior Management Team, and will develop appropriate actions and associated criteria by July 31, 2002.

3.   *Provide written guidance on the types of lost or stolen equipment, including items identified during physical inventories, which should be referred to the TIGTA's OI for investigation.*

We issued written guidance October 2001 in the TIGTA Operating Manual, Chapter 500, Section 140, which outlines the proper procedures for reporting all types of lost or stolen equipment. Augmenting this guidance, in-house training for all staff with inventory responsibility has commenced. In addition to instruction in the operation of the new PPM, this training will include awareness training in the application of TIGTA property management policy and employee responsibilities. We will complete training by September 30, 2002. Whenever an inventory item's status code is changed to reflect it has been reported missing, actions will be taken as determined by the TIGTA Board of Survey, including referral for full investigation.   The TIGTA PPMO is responsible for maintaining this guidance.

4.   *Ensure that periodic physical inventories are performed on the inventory of computers and that all discrepancies are resolved.*

Guidance added to the TIGTA Operating Manual, Chapter 500, Section 140, in October 2001, stipulates annual physical inventories will be conducted throughout the organization. In addition to conducting routine physical inventories, managers will be required to certify inventory lists of all items assigned to them and their staffs. The TIGTA Personal Property Management Officer will report any discrepancy to the Chief Information Officer and if necessary a meeting will be convened of the TIGTA Board of Survey. The TIGTA PPMO is responsible for assuring annual inventories and periodic inventory list review. We will conduct a comprehensive physical inventory beginning October 1, 2002.

Page 5

5. *Reinforce the guidelines to prepare Forms 1933 to consistently report lost or stolen items of inventory, or revise the guidelines if a comparable form of documentation is deemed appropriate.*

As stipulated in the guidelines of the Operating Manual update October 2001, TIGTA uses a process for consistently reporting and documenting lost or stolen items of inventory. The guidelines include how employees should report lost, stolen or damaged property. Potential disciplinary actions for lost or stolen items are outlined in the guidelines. The TIGTA Board of Survey will ensure consistent application of recommendations of disciplinary action across the functions. Guidelines in the TIGTA Operating Manual will be reinforced during the training mentioned above to assure consistency.

6. *Develop an encryption policy to reduce the risk of unauthorized disclosure of sensitive information maintained on laptop computers.*

TIGTA is participating in a Treasury information technology program piloting the use of Private Key Infrastructure (PKI) and smart cards. It is essential for the interoperability of our systems with the Treasury Department that we take advantage of this enterprise solution. Coincident with the pilot, that begins July 1, 2002, will be the development of an encryption policy to reduce the risk of unauthorized disclosure of sensitive information maintained on laptop computers. The pilot is designed to phase in operational activities, and TIGTA will implement the encryption policy bureau-wide by December 31, 2002. Appropriate training will be provided to TIGTA staff at the time of implementation. TIGTA's encryption policy will be the responsibility of TIGTA's Security Officer to assure integrity of our information technology systems. Further, the TIGTA security program is on the Office of Information Technology Program Status Review list, and TIGTA will regularly monitor the program status review list, and formally review it on a quarterly basis.

Page 6